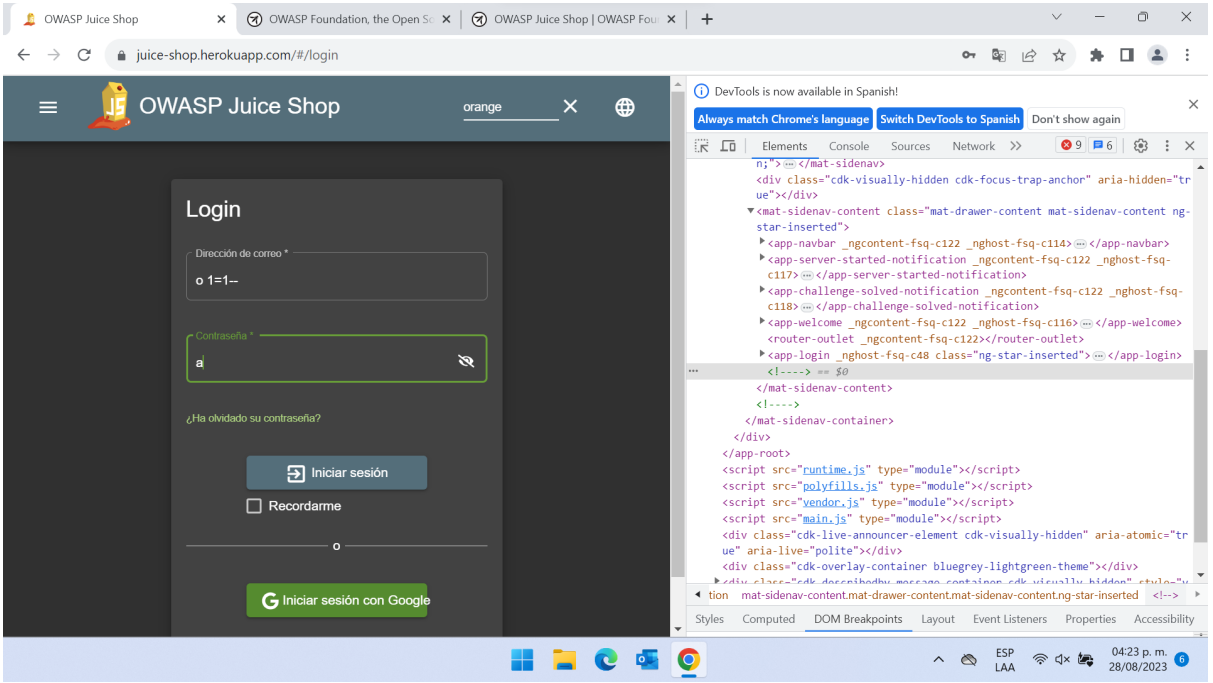
Actividad 6: Ejercicio de seguridad Aplicativa.

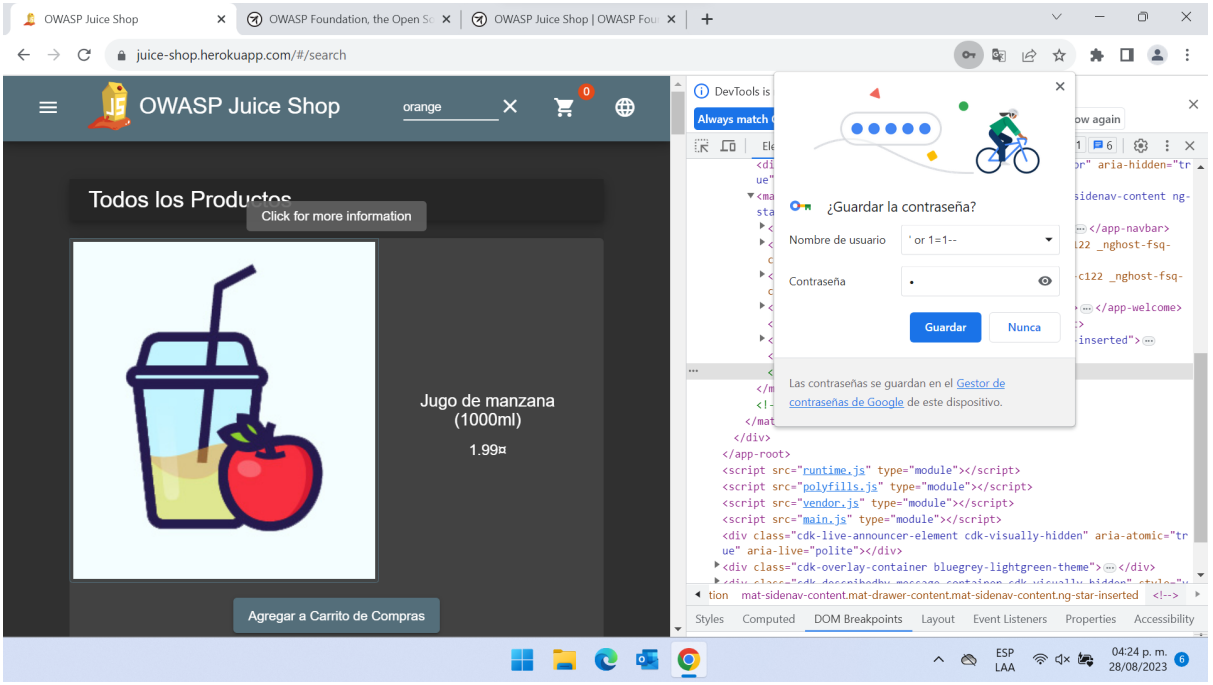
Equipo Solecito

Se está comprobando si el sitio sitio está protegido contra las amenazas comunes de OWASP Top Ten que son los 10 riesgos de seguridad más importantes en aplicaciones web las cuales enlistamos a continuación :

1. Inyección SQL (SQLi): Intenta ingresar datos maliciosos en formularios y URL para ver si el sitio es vulnerable a inyecciones SQL. Si obtienes resultados inesperados o errores de SQL, podría indicar una vulnerabilidad.}

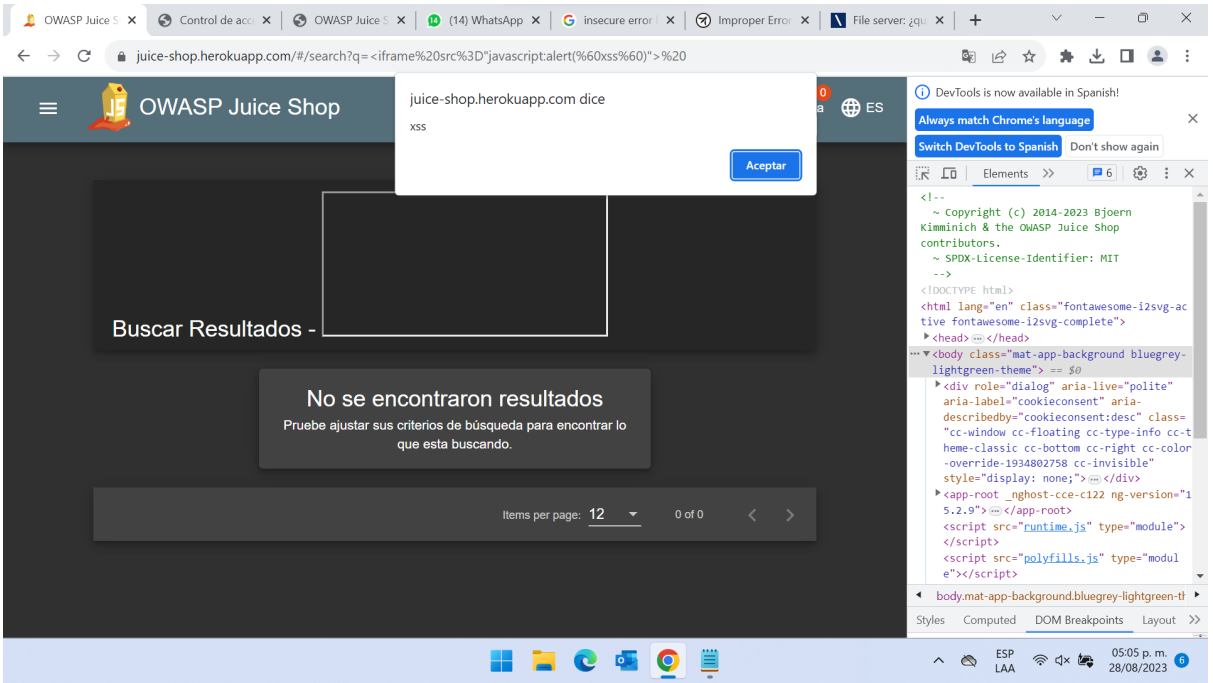
encontramos que se puede acceder a su admin con las siguientes credenciales
dirección de correo:' or 1=1--
contraseña:a





2. Cross-Site Scripting (XSS): Introduce scripts en campos de entrada (como formularios de búsqueda o comentarios) y observa si se ejecutan. Si el script se ejecuta en la página, es posible que haya una vulnerabilidad XSS.

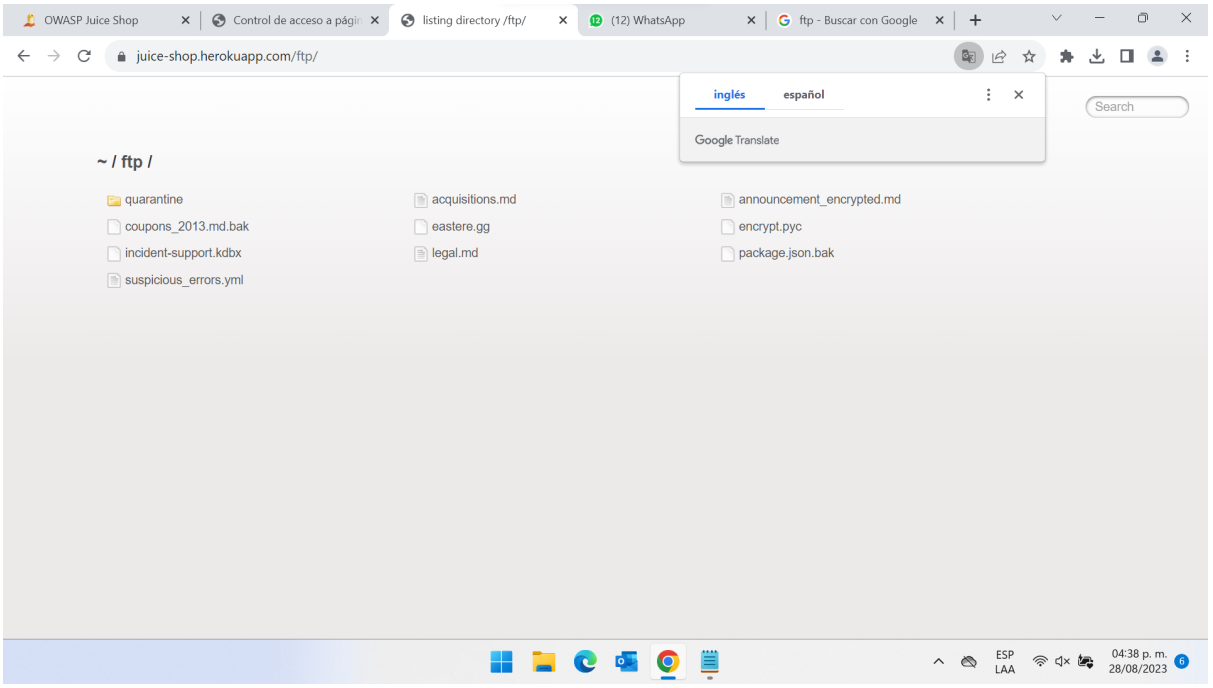
encontramos que en el buscador se puede ingresar lo siguiente y ejecutar el código javaScript <iframe src="javascript:alert(`xss`)">



3. Cross-Site Request Forgery (CSRF): Intenta realizar acciones en el sitio desde otra página sin que el usuario lo sepa. Si el sitio no utiliza medidas de protección, podrías ser vulnerable a CSRF.

4. Vulnerabilidades de Acceso: Verifica que las áreas restringidas del sitio requieran autenticación adecuada y no permitan el acceso no autorizado.

information disclosure: Directory list: dentro del la carpeta ftp en el archivo acquisitions existen documentos confidenciales:
https://juice-shop.herokuapp.com/ftp/acquisitions.md



- directory listing tiene expuesta su carpeta ftp de transferencia de archivos en sus términos y condiciones de uso
  https://juice-shop.herokuapp.com/ftp/

- Default page: página que nos describe sus vulnerabilidades
  https://juice-shop.herokuapp.com/#/score-board

  Control de acceso roto: Las restricciones en lo que los usuarios autenticados tienen permitido hacer en algunas ocasiones no se aplica de manera correcta. Los atacantes pueden explotar estas fallas para acceder a funcionalidades y/o datos no autorizados, como acceso a las cuentas de otros usuarios, archivos sensibles, modificar los datos de otros usuarios, cambiar permisos de acceso, etc.
  •Anti automatización descompuesta
  •Autenticación descompuesta
  •Problemas criptográficos
  •Validación de entrada incorrecta
  •Inyección
  •Deserialización Insegura
  •Varios
  •Configuración incorrecta de seguridad
  •Seguridad a través de la oscuridad
  •Exposición de datos sensible

•Redirecciones no validadas
•Componentes vulnerables
•XSS
•XxE

- Directory listing tiene expuesta su carpeta ftp de transferencia de archivos en sus términos y condiciones de uso:
  https://juice-shop.herokuapp.com/ftp/

- Insecure error handling: tiene un error 403 que puede bypasearse:
  https://juice-shop.herokuapp.com/ftp/coupons_2013.md.bak

  https://juice-shop.herokuapp.com/app/build/routes/fileServer

- default page
  https://juice-shop.herokuapp.com/app/build/routes/fileServer
  ctrl + u
  view-source:https://juice-shop.herokuapp.com/app/build/routes/fileServer